



Use of cause-consequence charts in practical systems analysis

Nielsen, Dan Sandvik

Publication date:
1974

Document Version
Publisher's PDF, also known as Version of record

[Link back to DTU Orbit](#)

Citation (APA):
Nielsen, D. S. (1974). *Use of cause-consequence charts in practical systems analysis*. Risø National Laboratory. Risø-M No. 1743

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Title and author(s) Use of Cause-Consequence Charts in Practical Systems Analysis	Date September 1974
	Department or group Electronic
	Group's own registration number(s) R-16-74
24 pages + tables + 7 illustrations	
Abstract The paper outlines the strategy and the main steps of cause-consequence analysis based on the concept of critical events. The so-called cause-consequence chart used for display in connection with cause-consequence analysis and for documentation purposes is described. Examples are given.	Copies to
	Abstract to

INTRODUCTION

Among the various faults that can arise during operation of a process plant, some will be relatively harmless, while others can lead to 'loss of production', 'damage to valuable plant components', 'injury to persons' etc. Activities associated with the planning, building, and operation thus include precautions against faults, so that the probability of various fault consequences is acceptable.

Examples of such protection activities are planning of fault detection and protection systems; planning of tests, inspection, and supervision; preparation of working instructions; and implementation of training and emergency exercises.

There are many cases of insufficient or faulty protection measures, or lack of protection, particularly when the plant is complicated or untraditional. When such plants are planned, consideration must be given not only to safety rules, norms, and procedures, but also to special plant conditions. Potential risk should be evaluated as part of a larger analysis of operations.

In a well designed plant, the probability of an incident or accident tends to be inversely related to the associated risk, and when dealing with the prediction of drastic consequences - as in safety analysis - great consideration should be given to the basic assumptions of the analysis, e. g. the influence from the human element of the system (Rasmussen (1)). A thorough analysis of risks demands co-ordinated collaboration between specialists from different fields. For example, engineers dealing with control and instrumentation must have access to detailed knowledge of the process itself, hereunder especially the chemical and physical properties of the converted materials, both under normal and abnormal operating conditions; and of the materials of plant construction.

Swift technological developments have implied that the designer can implement new system solutions with far more freedom than earlier. As a result he often has need for systematic and thorough decision-making to supplement the gradual accumulation of experience possible with traditional systems. To a certain extent, this need is filled by existing formalised methods, for example 'failure mode and effects analysis' (FMEA), 'fault tree analysis', or 'sneak circuit analysis' (Raskin (2)). Some such techniques

have been formalised to such an extent that computer-aid can be obtained. R. Taylor (3) presented a semi-automatic method for failure mode and effects analysis. Fussell (4) presented a formal method for constructing hardware-oriented fault trees for electrical systems. Powers (5) outlined a formal technique for safety analysis of chemical processes.

The user of a completed plant will largely judge its reliability performance on the costs resulting from faults in terms of loss of production, damage to plant, or injuries to staff. It is therefore important to develop systematic methods for cause-consequence analysis, relating the potential modes of failure to the ultimate consequences for the system.

For such failure/consequence analysis, the so-called cause-consequence chart (CCC) provides the engineer with both an analysis strategy, and a notation for presentation and documentation.

The CCC method is based upon the fact that the paths from several independent fault events pass to their consequences through focal nodes representing 'focal events', which very often have been identified during plant design. The 'focal events', therefore, will generally release some accident -preventing or -limiting action. By selecting expedient 'critical events' as 'focal events' a cause search, as well as a consequence search, will be facilitated in a systematic way.

Besides being used in connection with cause and consequence identification, the CCC offers a systematic support for probabilistic modelling (Nielsen and Runge (6)).

PRINCIPLES AND NOTATION

1. Starting the Analysis

On the highest level (plant level) the purpose of systematic cause-consequence analysis is to relate potential modes of failure of individual components to the ultimate consequences for the system ('loss of production', 'plant damage', etc.). In starting the analysis, however, the following question arises: What is an expedient starting point?

Starting the analysis with an arbitrary choice of an 'independent' potential fault, which does not directly affect the process, is inexpedient. Other faults may lead to the same consequences or the consequences may be harmless. A great deal of work may be wasted in this way. The potential number of trivial failures in a large process plant is very large.

For the high-risk faults (large potential cost of consequences) the direct effects will be that energy or mass balances of the main process are disturbed. This means that attention is naturally focussed on functional failures of process components that directly affect these balances and cause parameter changes/transients. It is here that the concept of a critical event becomes useful. A critical event is an unintended function of a component directly controlling or affecting main energy or mass balances, which can lead to significant consequences; or a breach of an energy or mass retaining boundary which can lead to significant consequences.

A functional failure which seems to be critical, or is known to be critical, may be chosen as the starting point for a search in which the potential causes of the event, and the potential consequences, are sought.

The designer often copes with several critical events by designing protective actions ('designed protective actions') which first occur when important process parameter limits are exceeded. This means that it may in some cases be expedient to start by selecting an event which is specified as 1) a radical abnormal change of a process parameter, e.g. feed water flow stops, or 2) a process variable exceeds a safety limit, e.g. 'pressure exceeds trip pressure'.

Starting with a change of a vital parameter, a cause search is initiated to find appropriate critical events. The cause-consequence analysis then proceeds from these critical events, unless it is evident that the identified critical events affect the process in nearly the same way. In the latter case, the parameter change itself, rather than any critical event, may be used as a starting point of the analysis.

The ability of the plant to meet and subdue excessive transients is largely determined by systems which 'as mentioned' are designed to perform accident preventing actions ('designed protective actions'). In this way undesired event sequences are prevented. However, a desired intervention may fail ('designed protective action x does not occur as intended') or it may not have been possible to design an intervention action at all. In such cases one must rely on accident-limiting systems (barriers, springler systems, evacuation, etc.).

2. The Cause-Consequence Chart

The display format used in connection with cause-consequence analysis

(based on the concept of critical events) is the cause-consequence chart (see symbols shown in appendix).

A CCC for a critical event describes the causes of the critical event and the different possible event sequences subsequent to it. The structure of a CCC for a critical event in some process system could be as shown in fig. 1.

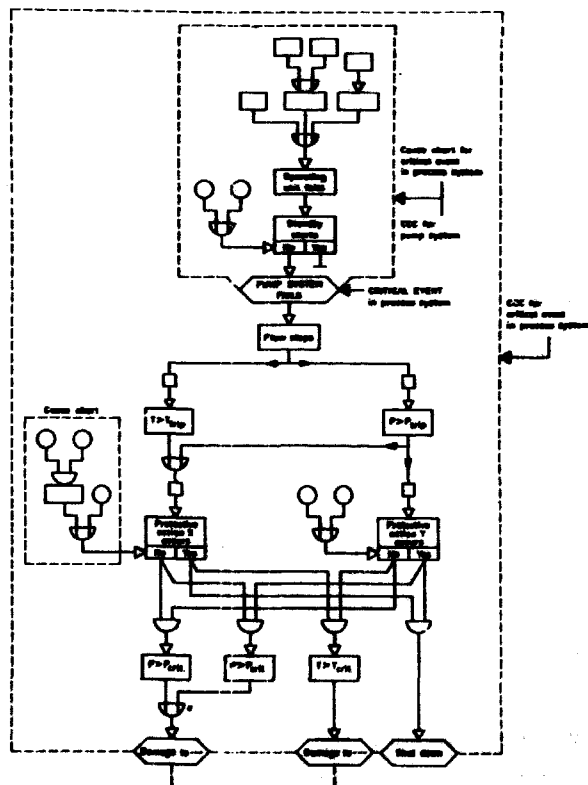


Fig. 1. The structure of a cause-consequence chart for a critical event in a process system.

A pump system consisting of two 100% full-load capacity pumps, one being a standby, may fail so that an important process flow stops. The critical event is "pump system fails".

In the consequence chart (below the focal node representing the critical event in fig. 1) different possible event sequences are described. Often a critical event can lead to different event sequences that may depend on conditions within the process system; in fig. 1 it is indicated that different event sequences can occur if, for instance, one or more of the accident-preventing actions ('designed safety actions') does not occur as intended. As the consequence chart provides the possibility for displaying the logical connection between events and conditions, different event sequences can be systematically identified.

An advantage of presenting sequences of events in a CCC is that the analyst is invited to study sequence. The sequence of events can be followed along the different paths in the block diagram.

Several cause charts may be attached to a consequence chart. A cause chart may be attached to describe possible causes of the critical event, i.e. the alternative prior sequences of events which can lead to the critical event, and the conditions under which these sequences can occur. In this way a focal node, representing the critical event, will appear in the chart. The initiating events which can lead to the critical event should be traced so far back that they can be considered as spontaneous and can be covered by statistical data.

Other cause charts attached to the consequence chart may be conventional fault trees, expressing the combination of conditions under which a certain event sequence in the consequence chart can take place.

Provided that the 'basic inputs' of the cause charts are independent, then the CCC displays the logical connection between a set of independent faults and their consequences.

As a CCC for a critical event describes one or more sequences of events, the time dimension is introduced in the chart. This provides, of course, the possibility of taking into account random faults that may occur in the time following the occurrence of the critical event; often a system with accident-limiting function is required to operate for a certain period (e.g. an emergency core cooling system in a nuclear reactor). The various 'independent' on-line faults of components that may occur during this period can be displayed in the consequence chart itself, or in an attached cause chart (i.e. a CCC can

cope with more operating phases of a system).

For a given limited system within a plant, thorough cause-consequence analyses will 'generate' a set of CCC's. The outputs of the CCC's for the system are significant consequences affecting the greater whole of which the system is a part (e.g. effect on production and economy).

Individual outputs from one or more CCC's for a given limited system may be the same specific consequence ('explosion in', 'no light', etc.), or may belong to the same category of consequences (e.g. various degrees of 'damage to system part x', or different duration of 'forced outage time'). Outputs from CCC's for a given limited system (or more limited systems) can therefore be inputs of cause charts for relevant critical events which disturb balances outside the system(s). This indicates the hierarchical structure of CCC's (consider, e.g. fig. 1 where the critical event 'pump system fails' is the output of a CCC for the pump system).

CAUSE-CONSEQUENCE ANALYSIS BASED ON THE CONCEPT OF CRITICAL EVENTS

A goal in all techniques of safety and reliability analysis is to provide a systematic procedure. The problem for safety analysis is especially difficult because the dynamic relationships between process parameters, and their transient effects on plant components are important; also event sequences of low probability, but with serious potential consequences, make the analysis much more complex.

The basic material for cause-consequence analysis is the plant hardware description in the form of functional system diagrams and flow sheets. These must be supplemented by physical layout drawings, observation of the actual hardware layout if this is possible; and with experience of component behaviour, especially in the later stages of the analysis. The formal requirements can be listed as follows:

1. Interconnection of plant components,
2. Location of systems, i.e. process components, systems with accident -preventing or -limiting functions, and auxiliary systems such as power, lubrication, cooling supplies, etc.,
3. Operating modes of systems,

4. Normal operating conditions for each component (in each mode) together with component limits for static and transient pressure, temperature, stress, and radiation loading,
5. Main process variables,
6. Energy sources and their location,
7. Physical and chemical properties of species under normal as well as abnormal operating conditions.

A review of the necessary detailed information of this kind for nuclear plant is presented by Garrick (7) and for chemical plant by Powers et al. (5).

Assume that this necessary information is available. Assume further that a dynamic model of the plant is available at least at the intuitive level. Some of the main steps in cause-consequence analysis are then:

1. Select a critical event (valid for a relevant operating mode).
Recall of the definition of a critical event: a critical event is an unintended function of a component directly controlling or affecting main energy or mass balances, which can lead to significant consequences; or a breach of an energy or mass retaining boundary, which can lead to significant consequences.
When selecting a critical event within the boundaries of a certain process system it is assumed that no other critical event has occurred within the system. Furthermore, it is assumed that the critical event will not occur due to normal operating effects from process parameters (pressure, temperature).
2. Modify the dynamic model taking the critical event into account, see fig. 2.
3. Specify the changes/transients (delay and magnitude) of the main process parameters at locations where there are protective devices or parts of protective devices (safety valves, sensors, etc.).
- 3a. Which trip limits/set points are exceeded ?
4. Are loading limits for relevant process components exceeded by effects from process parameter changes/transients ?
If so, a significant consequence may be another critical event, see fig. 2.

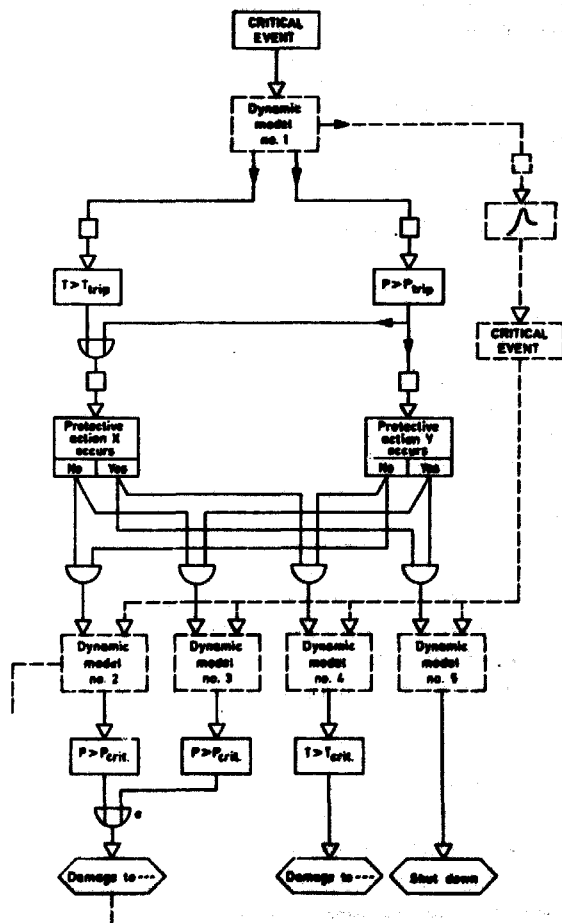


Fig. 2. Consequence analysis for critical event in a process system.

5. Identify the environmental changes within relevant areas, such as pressure /temperature/radiation changes, missile potentials, flooding, escape of species and perhaps phase changes of these.
A consequence of environmental changes may be a critical event in other structurally and operationally separate process systems.
- 5a. Identify potential transgression of trip limits/set points (due to environmental changes) at locations outside the main process where there are protective devices or parts of protective devices (safety valves, sensors, etc.)
- 5b. Are conditions present for fire/explosion in case of escaped species ? (e.g. temperature $> T_1$, pressure $> P_1$, concentration $> C_1$, and presence of ignition source).
If so, what are the potential, significant consequences ? ("damage to --, 'injury to staff').
- 5c. Identify accident-limiting barriers, if any, designed to cope with environmental changes.
- 5d. Do the environmental pressure and/or temperature changes/transients exceed the specified loading limits for the individual accident-limiting barriers, if any ?
If so, what are the potential, significant consequences ?
6. Identify which 'designed protective actions' (i.e. accident-preventing or -limiting actions) are potential according to the answers to items 3a and 5a ?
In this connection it should be realized that:
 - a) a designed protective action can, if released, be 'desirable' as well as 'undesirable' in the context of the actual accident situation.
 - b) a desirable designed protective action may fail (i.e. designed protective action x does not occur as intended).
7. Construct a consequence chart which shows the potential combinations of 'released' and 'not released' designed protective actions, see fig. 2.
8. For each combination identified in item 7 modify the dynamic model taking into account other critical events, if any (see item 4).
9. For each of the identified potential accidents specify the changes/transients

of main process parameters (pressure, temperature) in relevant process components (systems).

10. The following applies to each of the identified, potential accidents:
Are loading limits for relevant process components exceeded by effects from process parameter changes/transients ?
If so, what are the potential, significant consequences ? ('damage to ---', 'escape of ---', injury to ----).
 11. Continue the consequence search, if relevant, otherwise go to item 12.
-
12. Are significant consequences identified ?
If so, then proceed to item 13, otherwise go to item 1.
 13. Identify the potential causes of the critical event.
 - 13a. If the critical event is a failure mode of a 'static' component (pipe-line, flange, vessel, etc.), then:
Identify the potential influences of other structurally and operationally separate systems (e.g. effects of cranes, missiles, flooding, pressure, temperature, vibration, etc.).
 - 13b. If the critical event is a failure mode of an 'active' component (e.g., 'control valve x closes', or 'pump x fails') then:
Identify the relevant, functionally related units and their locations.
For each unit identify the relevant failure mode and the possible environmental effects which may cause it.
 - 13c. Display the result in a cause chart with reference to relevant information.
 14. Determine whether the individual system, which is called upon to perform a desirable accident-preventing or -limiting action, is capable of coping with the critical event, assuming that no faults in the system have occurred or occur during accident conditions. For instance, is the response time of the system adequate ?
If so, then proceed to item 14a.
 - 14a. Identify the potential 'in-system' causes of the failure 'designed protective action x does not occur as intended' (e.g., an 'unannounced' basic fault event has occurred).

- 14b. Identify environmental effects that may cause the failure 'designed protective action x does not occur as intended' during the course of an accident (e.g. influences of missiles, fire, flooding, humidity, temperature, pressure, radiation, vibration, etc.). Here there is a problem of identifying the causative factors of 'common mode failure', i.e. simultaneous failure of multiple units (e.g. redundant units) due to a common cause.
 - 14c. Display the result in a cause chart with reference to relevant information.
-
15. Redesign, if necessary.
 16. Go to item 1, if relevant, otherwise go to item 17.
-
17. Repeat the procedure for other structurally and operationally separate process systems within the plant.

PROBABILISTIC ANALYSIS

An Assessment of the probability of significant plant hazards may be highly desirable. A necessary basis for probabilistic analyses is that 1) thorough cause-consequence analyses have been performed, and that 2) the ability of 'safety systems' to cope with the various critical events have been substantiated during the analysis.

The probabilistic modelling techniques deal with component faults that can be considered as spontaneous and can be covered by significant statistical data. The effect of repair and test policy can be taken into account, if relevant. In connection with probabilistic failure modelling the CCC provides a systematic method of documentation (8).

EXAMPLES

Example 1

Fig. 3 shows an example of a simple process system in which light is produced. When the switch is closed, the relay contact closes and the contact of the circuit breaker opens. If the relay contact transfers open, the light will go out and the operator will 'immediately' open switch 8 which in turn

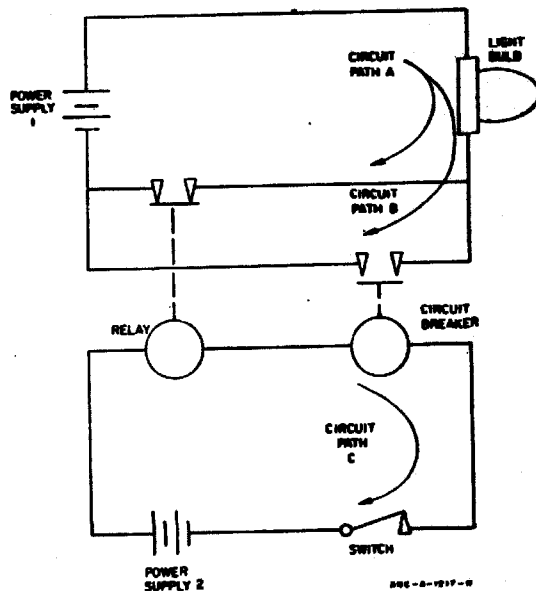


Fig. 3. System example.

causes the circuit breaker contact to close and restore the light. This example was used by Fussell (9) to demonstrate a method for obtaining the correct set of minimal cut-sets from a fault tree in which mutually exclusive faults appear. (A minimal cut-set in a fault tree is a collection of primary failures all of which are necessary and sufficient to cause system failure by that minimal cut set. A complete set of minimal cut-sets are all the unique failure modes for a given system and TOP event (Fussell (9)). Fussell points out that unless accounting properly for mutually exclusive faults that appear in the domain of the same AND-gate, erroneous minimal cut-sets can result.

The system example in fig. 3 is used here to illustrate, under non-dynamic

conditions, the procedure of cause-consequence analysis based on the concept of critical events.

In the normal operating mode of the system circuit paths A and C are 'active' and the vital process parameters are:

- 1) emf in circuit path A, and
- 2) emf in circuit path C.

The procedure of a cause-consequence analysis related to circuit path A can be summarized to:

1. Identify vital components in circuit path A.
2. Select a critical event.
3. Identify designed protective action, if any.
4. Construct a consequence chart which shows the sequence of events, and if relevant, focuses upon the failure 'designed protective action does not occur'.
5. Identify significant consequence.
Go to item 1, if relevant, otherwise go to item 6.
6. Identify, if relevant, causes of the failure 'designed protective action does not occur'.

Following this procedure we get three CCC's for the critical events h, i, and a, see fig. 4. The designer has coped with event a by designing the protective action 'circuit breaker contact closes'. The causes of the failure 'circuit breaker contact does not close' are f and g.

The same procedure of analysis can be used for circuit path C. It seems, however, in this case more expedient to start the analysis by selecting the event 'emf removed from circuit path C'. The procedure is then:

1. Identify designed protective action, if any.
2. Construct a consequence chart which shows the sequence of events, and, if relevant, focuses upon the failure 'designed protective action does not occur'.
3. Identify significant consequence.
4. Identify vital components in circuit path C.

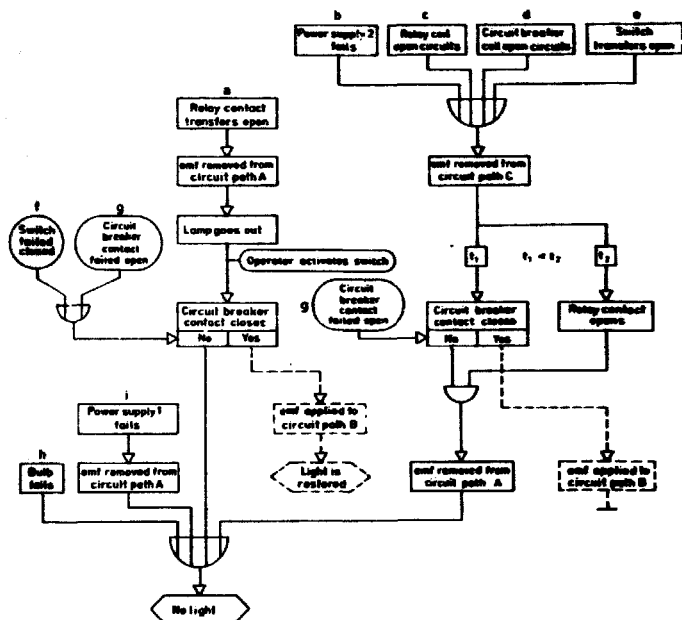


Fig 4. CCC for system example in Fig 3.

5. Identify causes of the focal event 'emf removed from circuit path C', i.e. identify the critical events in circuit path C.
6. Identify, if relevant, causes of the failure 'designed protective action does not occur'.

Following this procedure we get a single CCC which in fact is a combination of four CCC's for individual critical events which are b, c, d, and e. The designer has coped with the focal event 'emf removed from circuit path

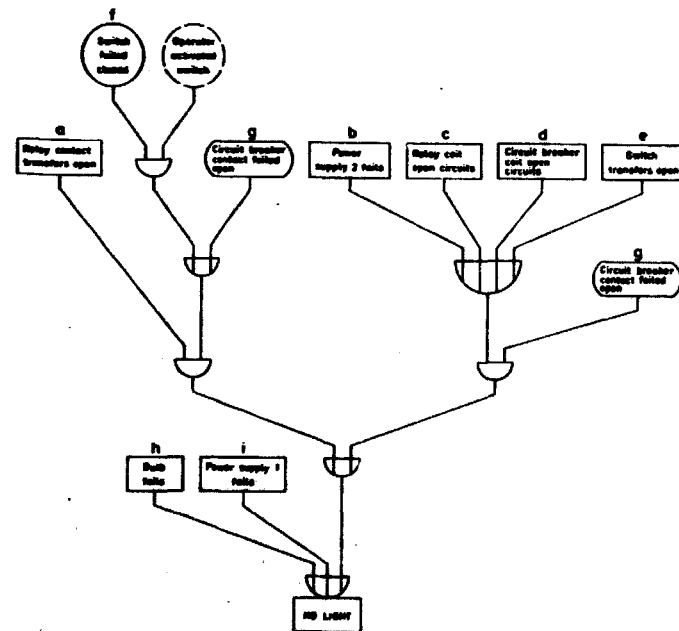


Fig. 5. Fault tree for system example in Fig. 3.

C' by the same protective action, i. e. 'circuit breaker contact closes'. The cause of the failure 'circuit breaker contact does not close' is g.

The total chart in fig. 4 can be considered as a CCC for the system in fig. 3 (in fact the chart is a combination of seven CCC's for individual critical events which are h, i, a, b, c, d, and e).

The Boolean expression for the corresponding fault tree is

$$h + i + a \cdot (f + g) + g \cdot (b + c + d + e), \text{ see fig. 5.}$$

(We find no erroneous minimal cut-sets in the tree. When using conventional fault tree analysis with the same system the mutually exclusive faults f and e will appear in the domain of the same AND-gate).

When analysing a 'two-state-type system', as that in fig. 3 or, for instance, a sequential control system, it is practical first to construct a functional diagram of the system. By using CCC-symbols for this purpose the consequence chart(s) for the system is almost 'automatically' generated. In the next example this is illustrated for a complex sequential control system.

Example 2

Consider fig. 1 where the event 'pump system fails' is a critical event in some process system. The cause chart for this critical event is a CCC for the pump system consisting of two 100% full-load capacity pumps, one being a standby. In the CCC for the pump system the focal event 'operating unit fails' is a critical event for the pump system. The designed protective action is 'standby starts'.

An evaluation of the probability that 'standby fails starting' on demand may be relevant in connection with an assessment of the probability of significant plant hazards. A thorough analysis of the conditions for a failing start-up must then be performed, i. e. a cause search is required for identifying, for instance component fault modes that can be considered as spontaneous and can be covered by statistical data. Such strict analysis requirements are, however, normally unnecessary in, e.g. analyses of alternative system designs aiming at an economical optimal solution. (In such preliminary analyses it is usually reasonable to ignore possible environmental effects on the components and assume similar operating conditions for the systems). The example to be considered here is related to the latter category of analysis, and stems from some analyses which have been carried out for alternative

boiler feed pumps systems.

One of the systems that was analysed is a system with two 100% full-load capacity pumps, one being a standby. Each pump is provided with a leak-off system and is driven by a slip ring motor with a liquid rheostat connected to the rotor.

The principle of the automatic sequential control system for start-up and shut-down of a pump group is shown in fig. 6. The pump groups are controlled by a master controller; if a running pump group fails, the master controller demands start-up of the standby and, provided that the plant criteria are fulfilled, the main motor is switched in.

Each pump runs for one week and is then shut down for one week. In the shut-down period maintenance of slip rings and the slip ring house is carried out. If a demand occurs during this period, the maintenance is interrupted and the standby is re-established.

In order to identify causes of 'standby fails starting' it is expedient first to construct a functional diagram showing all the 'designed events' that are established to carry out the designed protective action 'standby starts'. In so doing the various vital functional units and components, often shown in several complex electrical diagrams, can be systematically identified. By using CCC-symbols when constructing the functional diagram a consequence chart is generated at the same time, see fig. 7.

The next step in the analysis is then to identify the causes of a failing start-up.

The causes of a failing start-up can be divided into two categories - those that occur or appear during the start-up phase itself, and those that have already taken place before demand. As far as the latter category is concerned there may sometimes be a 'dead time' during the scheduled shut-down period of a pump in which the pump, i. e. the standby, is incapable of being started because of:

1. Presence of an unannounced fault.
 2. Scheduled maintenance during the standby period of a pump.
- or because it is undergoing:
3. Repair of a announced fault (mainly faults in operating lubrication and cooling systems).

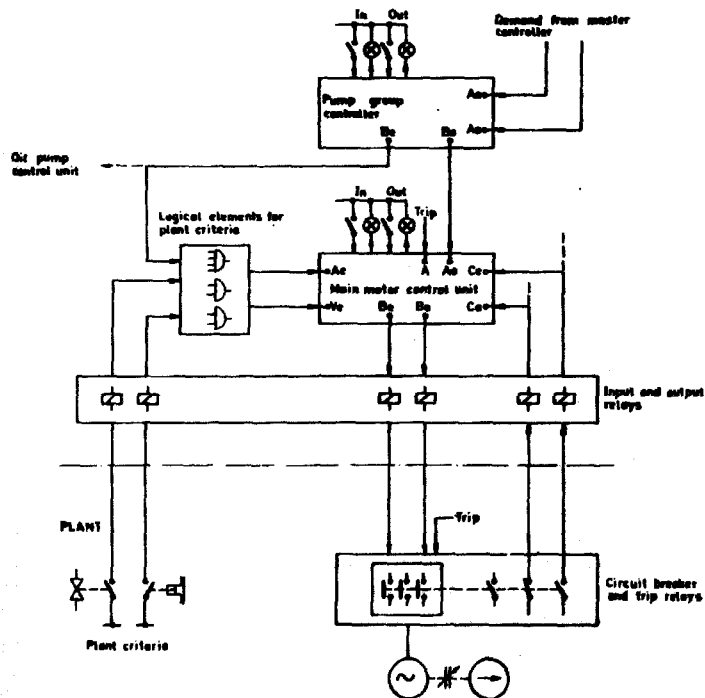


Fig. 6. Sequential control system for start-up and shut-down of a pump group.

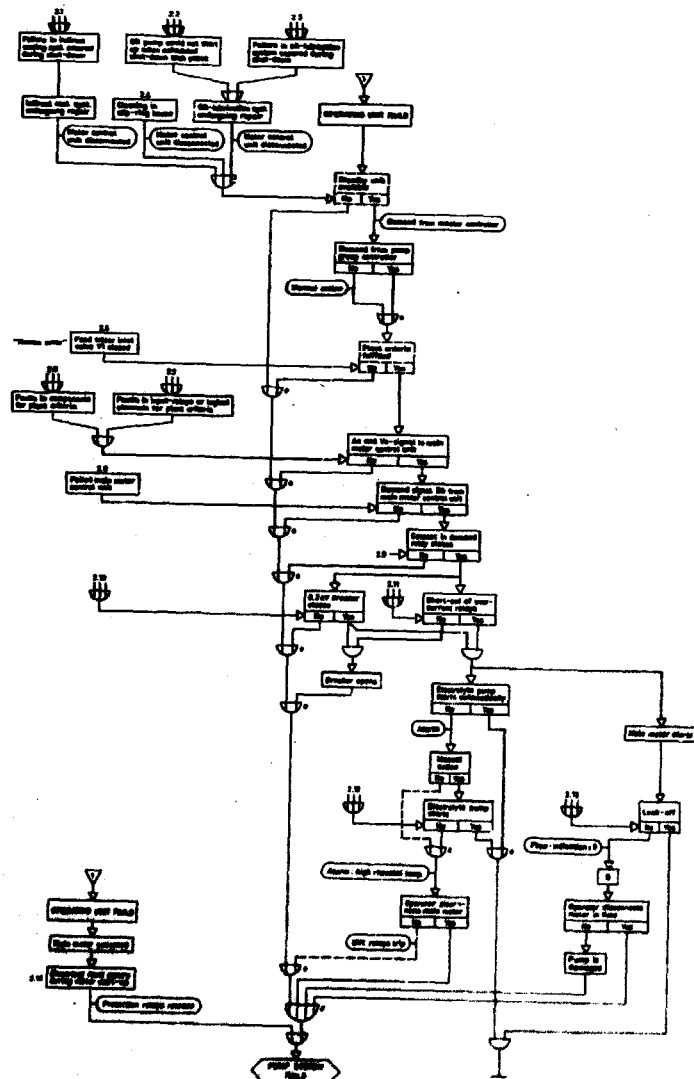


Fig. 7. GOTO-computer chart for pump system.

4. Repair of an unannounced fault that is disclosed by the scheduled change over.

The total CCC for the pump system, see fig. 7, indicates the various kinds of causes of the failure "pump system fails".

CONCLUDING REMARKS

The present paper has described the strategy and the main steps of cause-consequence analysis based on the concept of critical events. The emphasis has been placed on application of the analysis strategy and the display format, the cause-consequence chart (CCC), to technical process systems.

The same principle of analysis strategy may be used when analysing other types of problems involving potential disturbances of vital balances (e. g. ecologic and economic balances).

The method has been applied in practice to several power plant systems at a detailed level. Future developments anticipated include semi-automation of CCC construction, and more detailed definition of the kind of component reliability models required for realistic systems analyses, such as those provided by studies of reliability physics.

REFERENCES

- 1) Rasmussen, J., "The Role of the Man-Machine Interface in Systems Reliability", NATO Advanced Study Inst. on Generic Techniques of System Reliability Assessment. Risø-M-1673, (1973).^{1, 2}
- 2) Rankin, J. P., "Sneak-Circuit Analysis", Nuclear Safety, vol. 14, no. 5, Sep.-Oct. 1973.
- 3) Taylor, R., "A Semiautomatic Method for Qualitative Failure Mode Analysis", CSNI Specialist Meeting on The Development and Application of Reliability Techniques to Nuclear Plant. Risø-M-1707, (1974).¹
- 4) Fussell, J. B., "Synthetic Tree Model - A Formal Methodology for Fault Tree Construction", ANCR-1098, (1973).³
- 5) Powers, G. J. and Tompkins, F. C., "Fault Tree Synthesis for Chemical Processes", AIChE Journal, vol. 20, no. 2, 1974.
- 6) Nielsen, D. S. and Runge, B., "Unreliability of a Standby System with Repair and Imperfect Switching", IEEE Transactions on Reliability, vol. R-23, no. 1, April 1974.
- 7) Garrick, B. J. "Principles of Unified Systems Safety Analysis", Nucl. Eng. Des., vol. 13, Aug. 1970.
- 8) Nielsen, D. S., Platz, O., and Runge, B., "A Cause-Consequence Chart for a Redundant Protection System". To be published in IEEE Transactions on Reliability.
- 9) Fussell, J. B., "Fault Tree Analysis - Concepts and Techniques", NATO Advanced Study Inst. on Generic Techniques of System Reliability Assessment.²

¹ Available from the Library of the Danish Atomic Energy Commission, Risø, DK-4000 Roskilde, Denmark.

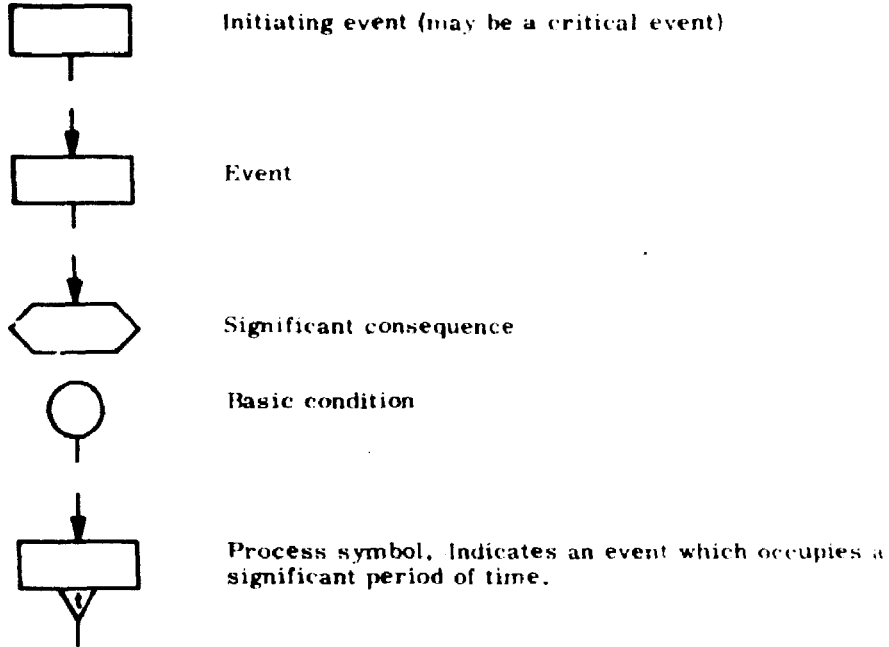
² To be published by Nordhoff Publishing Company.

³ Available from the NTIS, Springfield, Va. 22151.

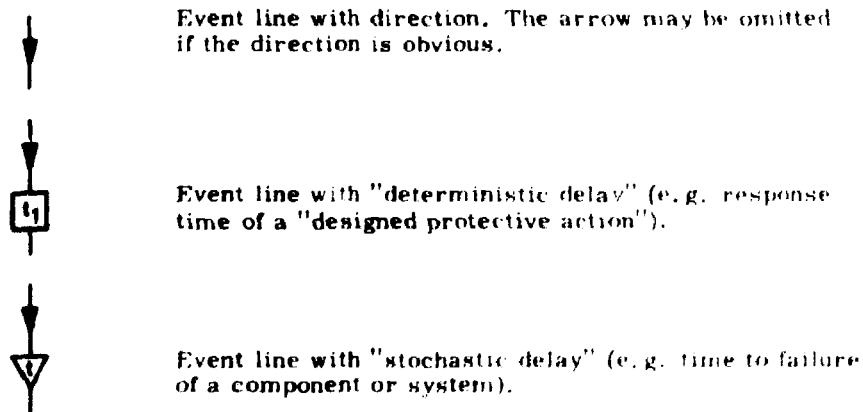
APPENDIX

Description of the symbols in the cause-consequence chart

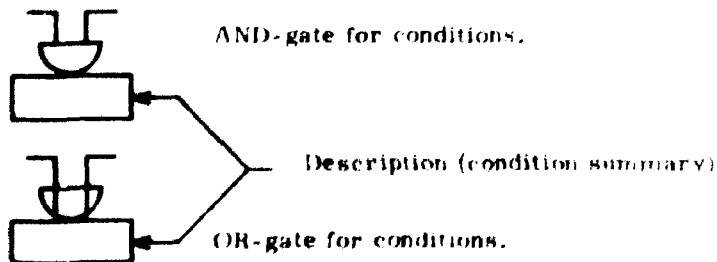
1. Events



2. Event lines



3. Condition gates



4. Gates for combining several event lines



Inclusive OR-gate for "join" of two event sequences.



Exclusive OR-gate for "join" of two event sequences.

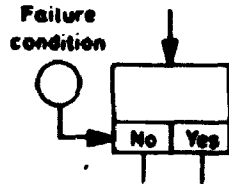


AND-gate for event sequences.

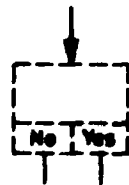
5. Vertices for event lines



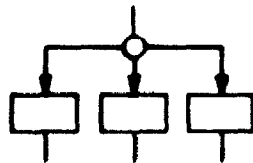
AND-vertex. The event propagation will continue in both directions.



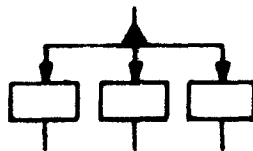
Either/or-vertex. The vertex describes a "designed action/event". The event propagation follows the No-output if a failure condition is present.



Condition-vertex. The vertex describes a condition. The event propagation follows the No-output if the condition is not fulfilled.



Mutually exclusive, exhaustive OR-vertex for events.



Mutually exclusive OR-vertex for spontaneous events. The event propagation moves in one of the directions indicated. This symbol follows either stochastic time delay or process symbols.

6. Messages

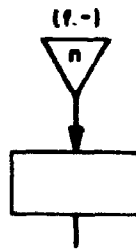


Condition which is assumed to be fulfilled — comment.

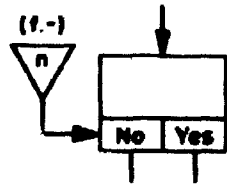
7. Transfer symbols and possibilities for attachment of cause charts.



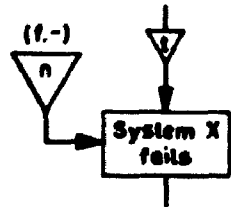
Symbol for cause chart.



Cause chart n for critical event; may be shown separately in fig. -.



Cause chart n (condition tree); may be shown separately in fig.-.



Cause chart n (event tree) for the spontaneous event "system x fails" (specified on-line failure mode); may be shown separately in fig.-.



Out-transfer. The event line is continued at the corresponding in-transfer symbol (a) at another place in the diagram (or in fig. -).



In-transfer. The event line continues from the corresponding out-transfer symbol (a) (in the diagram or in fig. -).